(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 December 2002 (19.12.2002)

PCT

(10) International Publication Number
WO 02/102075 A1

(51) International Patent Classification[7]: H04N 7/16, 7/167

(21) International Application Number: PCT/IB02/02138

(22) International Filing Date: 6 June 2002 (06.06.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
01202194.5 8 June 2001 (08.06.2001) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SCHIPPER, Robert** [NL/NL]; Internationaal Octrooibureau B.V., Prof . Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agent: **DUIJVESTIJN, Adrianus, J.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

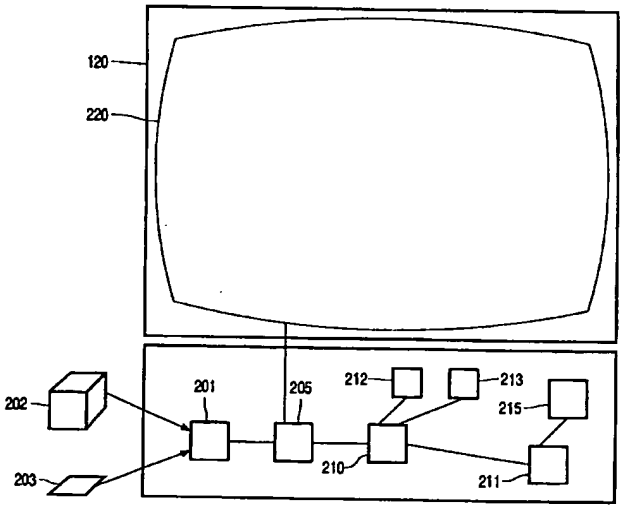
(81) Designated States *(national)*: CN, JP, KR, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DEVICE AND METHOD FOR SELECTIVELY SUPPLYING ACCESS TO A SERVICE ENCRYPTED USING A CONTROL WORD, AND SMART CARD



(57) Abstract: Device (120), smart card (300) and method for selectively supplying access to a service (202) encrypted using a control word. A service (202) is received with an entitlement control message (ECM) (203) comprising authorization data and a specifier of a validity period of the authorization data. The service is decrypted only if the ECM (203) is found valid. The service (202) can be stored on a storage medium such as a DVD. An ECM transcoding module (211) obtains the authorization data from the ECM (203) supplies to writing means (215) a device-specific ECM comprising the authorization data. The device-specific ECM may be encrypted with a key specific to the device (120) and/or comprise an identifier for the device (120).

WO 02/102075 A1

Device and method for selectively supplying access to a service encrypted using a control word, and smart card

The invention relates to a device for selectively supplying access to a service encrypted using a control word, comprising receiving means for receiving the service and an entitlement control message (ECM) comprising authorization data and a specifier of a validity period of the authorization data, decrypting means for decrypting the service using the control word, a timer for providing a time, and conditional access means for obtaining the authorization data and the specifier of the validity period of the authorization data from the ECM and providing the control word to the decrypting means in dependence on a verification of the authorization data and on a determination of the time being within the validity period.

The invention further relates to a method of selectively supplying access to a service encrypted using a control word, comprising receiving the service and an entitlement control message (ECM) comprising authorization data and a specifier of a validity period of the authorization data, providing the control word in dependence on a verification of the authorization data and on a determination of the time being within the validity period obtained from the CM, and decrypting the service using the control word.

A device according to the preamble is known from United States Patent 6,005,938. Service providers, such as subscription-based television providers, typically protect information which they distribute as part of their service from being accessed by users who have not paid for the service by encrypting that information. User who want to access the service must obtain a so-called entitled control message (ECM) comprising authorization data in order to access the service. The ECM will typically comprise a control word or decryption key which can be used to decrypt the encrypted service. Alternatively, the control word can be stored in a smart card which the user has bought before and which he needs to insert in his television or set-top box. In that case, the ECM comprises authorization data which causes the smart card to provide the control word to the decryption module. Using the control word, the decryption module can decrypt the service and allow the user to access it. This way the user can view the subscription-based television or access an interactive service.

In such an arrangement, a user could record an ECM which he receives from the service provider, and use it again in order to access the service once again. This allows him to access the service without paying for it. To prevent this, the service providers often insert a specifier of a validity period of the ECM in the ECM. The smart card or set-top box which receives the ECM will check the specifier or the validity period against the time at which the user wants to access the service and refuse to provide the control word to the decrypting module if the current time falls outside the validity period.

For some applications, local storage of the information related to the service is required. For example the user may want to record a television program provided through the subscription-based television service so that he can view it later at his convenience. However, if the information is stored in a plain form, access control is gone. In order to make sure that the access control stays intact, the information is stored in the encrypted format. In order to allow the user to later access the stored information the ECM needs to be stored as well. However, because of the specifier of the validity period of the ECM, the stored information may become inaccessible when the user wants to play it after the validity period has expired. This means that the user cannot access the information he bought at the time he chooses.

It is an object of the invention to provide a device according to the preamble, which is more flexible with regard to providing access to the service.

This object is achieved according to the invention in a device which is characterized by ECM transcoding means for obtaining the authorization data from the ECM and for supplying to writing means a device-specific ECM comprising the authorization data. By creating a device-specific ECM it becomes possible to access the stored services or information at any moment because the device-specific ECM does not comprise a validity period.

In an embodiment the conditional access means are arranged for providing the control word if it is present in the authorization data. This way the device does not need to store the control word in the secure storage somewhere but can simply obtain the control word from the authorization data in the ECM.

In a further embodiment the ECM transcoding means are comprised in a smart card. It is desirable to have the conditional access means stored in a secured fashion so that malicious users cannot temper with them. The same of course goes for the ECM transcoding

means. By putting these means in a smart card it becomes much harder for a malicious user to temper with it in order to obtain device-specific ECMs for other devices.

In a further embodiment the device-specific ECM comprises an identifier for a group of devices, the device being an element of said group. A greater flexibility can be obtained by not restricting the device-specific ECM to one particular device. Instead the device-specific ECM can be provided with a group identifier or a number of identifiers of specific devices. This allows the user to, for example, record the encrypted service on one device and to play it back on another device.

In a further embodiment the device-specific ECM comprises an identifier for the device. In order to prevent the user from using that device-specific ECM at another device, an identifier for the device is recorded in the device-specific ECM. This way the user can only use the device-specific ECM at that particular device.

In a further embodiment the device-specific ECM is encrypted with an encryption key for which the device has a corresponding decryption key. By encrypting the device-specific ECM, the user will be unable to access the device-specific ECM using any device other than the one in which the device-specific ECM has been created. This protects against copies of the device-specific ECM being distributed to unauthorized third parties.

It is a further object of the invention to provide a method according to the preamble, which provides more flexibility with regard to supplying access to the service.

This object is achieved according to the invention in a method which is characterized by the step of obtaining the authorization data from the ECM and for supplying to writing means a device-specific ECM comprising the authorization data. By creating a device-specific ECM it becomes possible to access the stored services or information at any moment because the device-specific ECM does not comprise a validity period.

It is a further object of the invention to provide a smart card for use in a device according to the invention which provides greater flexibility in the device with respect to providing access to the service.

This object is achieved according to an invention in a smart card which is characterized by ECM transcoding means for obtaining authorization data from an ECM and for supplying to writing means a device-specific ECM comprising the authorization data. By storing the ECM transcoding means on a smart card a greater level of security for the ECM transcoding means is achieved. Further the user can use his smart card with any device that can receive it and so is not restricted to one particular device having ECM transcoding means.

In an embodiment the smart card further comprises conditional access means for obtaining a specifier of a validity period of the authorization data from the ECM and providing a control word to decryption means in dependence on the verification of the authorization data and on a determination of the time being within the validity period. By providing the conditional access means on the smart card as well it is achieved that the smart card can be used as a single conditional access mechanism which can be used in any device that is equipped with smart card reading means.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiment shown in the drawings in which:

Fig. 1 schematically shows an arrangement according to the invention comprising a service operator and a receiving device;

Fig. 2 schematically shows the device according to the invention in more detail; and

Fig. 3 schematically shows a smart card according to the invention in more detail.

Throughout the figures same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represents software entities such as software modules or objects.

Fig. 1 schematically shows an arrangement 100 comprising a service operator 101 and a receiving device 120 connected via a network 110 such as the Internet or a cable television network. Using the network 110 the service provider 101 can provide instances of a service to the receiving device 120, for example by allowing the user of the receiving device 120 to access a subscription-based television service. The receiving device 120 can take many forms, such as a set-top box, a television, a radio, a personal computer and so on. The service provider 101 can provide the service in many ways. In some cases the service provider broadcasts the encrypted service to all receiving devices which are connected via the network and only receiving devices having the appropriate descrambling means can descramble and access the service. In other cases, the service provider 101 only provides

instances of the service, such as a specific movie or television program to a specific subscriber who has asked for it.

Typically the user of a receiving device 120 should only be able to access the service if he has paid for it. In order to restrict access, the service provider 101 encrypts the service or the instances thereof which he distributes to the receiving device 120. The user of the receiving device 120 must then obtain the appropriate control words necessary to decrypt the service. There are many ways in which the distribution of control words to the users can be facilitated. The control word can be stored in the receiving device 120 or it may be distributed by the service provider 101 to the receiving device 120 upon a payment from the user. The control word can be distributed via the network 110 or be stored on a smart card which the user can insert in the receiving device 120.

If the control word is stored in the receiving device 120 authorization must be sent by the service provider 101 to the receiving device so that it will use the control word to access the service. If no authorization is received the receiving device must refuse to decrypt the service. The authorization is distributed in the form of a so-called entitlement control message (ECM). Upon receipt of a valid authorization for accessing the service the device uses the control word to provide the user access to the service. If the control word is not available in the receiving device 120 itself, and not made available on a smartcard either, the service provider 101 must send the control word as a part of the ECM.

Fig. 2 shows the receiving device 120 in more detail. The device comprises a receiving module 201 which receives a service or an instance thereof 202 and an ECM 203 from the service provider 101. The instance 202 is fed to a decrypting module 205 which decrypts the instance 202 using a control word and feeds the decrypted instance to a rendering module 220 such as a television screen. This way the user can access the service or view the instance 202.

The control word is provided to the decryption module 205 by a conditional access module 210. The conditional access module 210 obtains authorization data and a specifier of the validity period of the authorization data from the ECM 203. First the conditional access module 210 checks the validity of the authorization data. The service provider 101 might for instance digitally sign the ECM 203 and then the conditional access module 210 verifies the digital signature. Additionally, it may need to check that the ECM 203 is indeed intended for use with the received instance 202.

Further, the conditional access module 210 needs to verify that the ECM 203 is still valid. The device 120 is to this end provided with a timer 212, such as a real time

clock, which provides the current time to the conditional access module 210. The conditional access module 210 then makes a determination whether the time is within the validity periods as indicated in the ECM. The validity period can be specified in the ECM 203 as a combination of a beginning or end date by a date and a valid representing a period of time or simply by a value representing a period of time. Additionally the validity period may specify a period in which the user may not receive the instance of the service.

If the conditional access module 210 finds that the ECM 203 is valid and that the current time is within the validity period, the conditional access module 210 provides the control word to the decrypting module 205. The control word may be present in the ECM 203 or it may be stored in the device 120 itself.

The user of the device 120 may want to store the received instance 202 on a storage medium such as a hard disk, DVD+RW or CD-RW. To this end, the device 120 comprises a writing module 215 such as a video recorder, a Digital Versatile Disc (DVD) writer, or a compact disc (CD) writer. This allows the user to save the received instance for later viewing. The writing module 215 must also store the authorization data present in the ECM 203. Storing the received instance 202 may require permission from the service operator 101. This permission could e.g. be given in the ECM 203 itself, or in another entitlement message.

If the control word is present in the ECM 203, then also the control word needs to be stored on the storage medium. Without the control word, it is impossible to access the stored instance 202. The instance 202 is stored in encrypted form.

An ECM transcoding module 211 obtains the authorization data from the ECM 203 and supplies to the writing module 215 a device-specific ECM which comprises the authorization data. Since the device-specific ECM does not comprise a specifier or a validity period the validity of the device-specific ECM is unlimited. This way, the user can play back the instance at any time he chooses which makes this device very flexible.

However, it is desirable that the authorization data stored in the device-specific ECM is protected in some way against unauthorized usage. For example, the user may make copies of the device-specific ECM from the storage medium and distribute those, so many people can access the stored instance. Since the service operator 101 normally charges every user for access, this is undesirable.

There are various ways in which the device-specific ECM can be protected against such misuse. In a preferred embodiment, the device-specific ECM further comprises an identifier for the device 120. When at a later time the receiving module 201 receives the

instance 202 from the storage medium, the conditional access module 210 will obtain the authorization data stored in the device-specific ECM, which authorization data comprises the identifier for the device. The conditional access module 210 then compares the identifier for the device as stored in the device-specific ECM with an identifier for the device 120. If the two identifiers match, the conditional access module 210 provides the control word stored in a device-specific ECM to the decrypting module 205.

The identifier for the device can also be realized as an identifier for a group of devices as long as device 120 is an element of said group. The conditional access module 210 then must verify that the device 120 is a member of the group when the device-specific ECM is provided to it.

To protect the device-specific ECM against misuse, it may be encrypted with an encryption key for which the device 120 has a corresponding decryption key. That way, only the device 120 will be able to decrypt the encrypted device-specific ECM and access the authorization data therein. This can be realized with public key cryptography, although of course also secret-key schemes can be used. A public/private key pair is stored in the device 120. The ECM transcoding module 211 accesses the public part of the key pair and encrypts the device-specific ECM with it. Later, the conditional access module 210 accesses the private part of the key pair and decrypts the device-specific ECM therewith.

The device 120 may comprise an decryption module 213, in which at least the private part of the key pair is stored. This way, malicious users cannot make a copy of the private part to decrypt the encrypted device-specific ECM and illegally access the authorization data. The decryption module 213 may be arranged to decrypt the encrypted device-specific ECM itself, or to provide the conditional access module 210 with the private part of the key pair when necessary.

The decryption key may be unique for the device 120, so that only the device 120 can access the authorization data. It may also be shared by a group of devices, whereby the device 120 is a part of that group. This allows the authorization data to be stored by one device and accessed by another device of the group.

Multiple copies of the device-specific ECM may be stored, each copy encrypted once for every device that is permitted to access it. Each of these devices can then access its own copy, but other devices cannot access the device-specific ECM.

In a further embodiment, the service provider 101 activates an "identify receiver" option. This option is present in the private CA parameters of the ECM 203. The option contains an AND mask and/or an OR mask. When present, the masks are used to mask

the unique identification pattern of the receiving device to allow for group access. In this embodiment, it is required that each receiving device has a unique identification pattern or identifier.

To generate the group identification, the ECM transcoding module 211 applies the AND-mask and the OR-mask to the device identifier for the receiving device 120. For example, the group identifier can be calculated as (device identifier AND AND-mask) OR OR-mask.

The ECM transcoding module 211 then combines the group identifier with the above-mentioned encryption key to generate an encryption key for encrypting the device-specific ECM. The device-specific ECM then contains the original AND and/or OR masks, and the encryption key result.

The encryption key for encrypting the device-specific ECM is preferably concatenated with the group identifier and fed to a hashing function. Output of the hashing function is a diversified key which is used for checking, generating, decrypting and encrypting of the device-specific ECM. An advantage of this approach is that this device-specific ECM can now be used immediately by any device within the group. Further, by using the hash function the length of the output does not depend on the length of the input.

Fig. 3 shows a smart card 300 comprising the conditional access module 210, the ECM transcoding means 211 and a secure storage module 301. Since the conditional access module 210 and the ECM transcoding module 211 deal with the authorization data and in effect provide the user with access to the service, they must be secured as much as possible. An effective way to protect these modules is to embody them on a smart card. Smart cards are much more difficult to compromise than ordinary computers or software and so offer a better way of protecting the conditional aspects of the conditional access service. The device 120 is then equipped with a smart card reading module 310, in which the user can insert the smart card 300. The smart card reading module 310 also facilitates the communication between the receiving module 201 and the decrypting module 205 embodied in the device 120, and the conditional access module 210 and the ECM transcoding module 211 embodied in the smart card.

The control word necessary to decrypt the service can be stored in the secure storage module 301 on the smart card. This way, it is very difficult for the user to obtain the control word, and so it is very difficult for him to access the service without paying for it.

It is possible that the device 120 has been tampered with in such a way that it will not simply decrypt the service, but instead store the control word or store the

unencrypted service without the permission from the service provider 101. In order to prevent such a modified device from accessing the control word, the smart card 300 may employ an authentication mechanism in order to verify whether the device 120 has been tampered with. This authentication mechanism is for instance realized by having the smart card issue an encrypted 'challenge' to the device 120, which the device 120 must decrypt and send back to the smart card 300. If the device 120 cannot correctly decrypt the challenge, it is not an compliant device and may not get access to the control word. Alternatively, the smart card 300 can check the integrity of some part of the program code to be executed by the device 120, for example by verifying a digital signature.

If the control word is not stored in secure storage module 301, but instead is provided in the ECM 203, the ECM 203 is provided to the smart card 300 and thereby to the conditional access module 210, which obtains the control word from the ECM 203. The control word will often be present in an encrypted form in the ECM 203, and so the conditional access module 210 will need to decrypt the control word first. The decryption key necessary to decrypt the control word can then be stored in a secure storage module 301.

The smart card 300 in a further embodiment further comprises the decryption module 213. This allows the user to access the encrypted device-specific ECM on any device with which he can use the smart card 300. The encryption key used to encrypt the device-specific ECM then needs to be one for which the corresponding decryption key is available in the decryption module 213.

CLAIMS:

1. A device for selectively supplying access to a service encrypted using a control word, comprising

receiving means for receiving the service and an entitlement control message (ECM) comprising authorization data and a specifier of a validity period of the authorization data,

decrypting means for decrypting the service using the control word,

a timer for providing a time, and

conditional access means for obtaining the authorization data and the specifier of the validity period of the authorization data from the ECM and providing the control word to the decrypting means in dependence on a verification of the authorization data and on a determination of the time being within the validity period,

characterized by

ECM transcoding means for obtaining the authorization data from the ECM and for supplying to writing means a device-specific ECM comprising the authorization data.

2. The device of claim 1, whereby the conditional access means are arranged for providing the control word if it is present in the authorization data.

3. The device of claim 1, whereby the ECM transcoding means are comprised in a smartcard.

4. The device of claim 1, whereby the device-specific ECM comprises an identifier for a group of devices, the device being an element of said group.

5. The device of claim 1, whereby the device-specific ECM comprises an identifier for the device.

6. The device of claim 1, whereby the device-specific ECM is encrypted with an encryption key for which the device has a corresponding decryption key.

7. A method of selectively supplying access to a service encrypted using a control word, comprising

receiving the service and an entitlement control message (ECM) comprising authorization data and a specifier of a validity period of the authorization data,

providing the control word in dependence on a verification of the authorization data and on a determination of the time being within the validity period obtained from the CM, and

decrypting the service using the control word,

characterized by obtaining the authorization data from the ECM and for supplying to writing means a device-specific ECM comprising the authorization data.

8. A smartcard for use in the device of claim 1, characterized by

ECM transcoding means for obtaining authorization data from an ECM and for supplying to writing means a device-specific ECM comprising the authorization data.

9. The smartcard of claim 8, further comprising

conditional access means for obtaining a specifier of a validity period of the authorization data from the ECM and providing a control word to decrypting means in dependence on a verification of the authorization data and on a determination of the time being within the validity period.

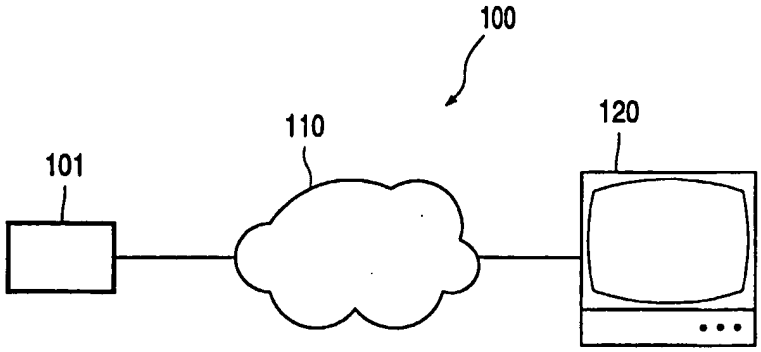


FIG. 1

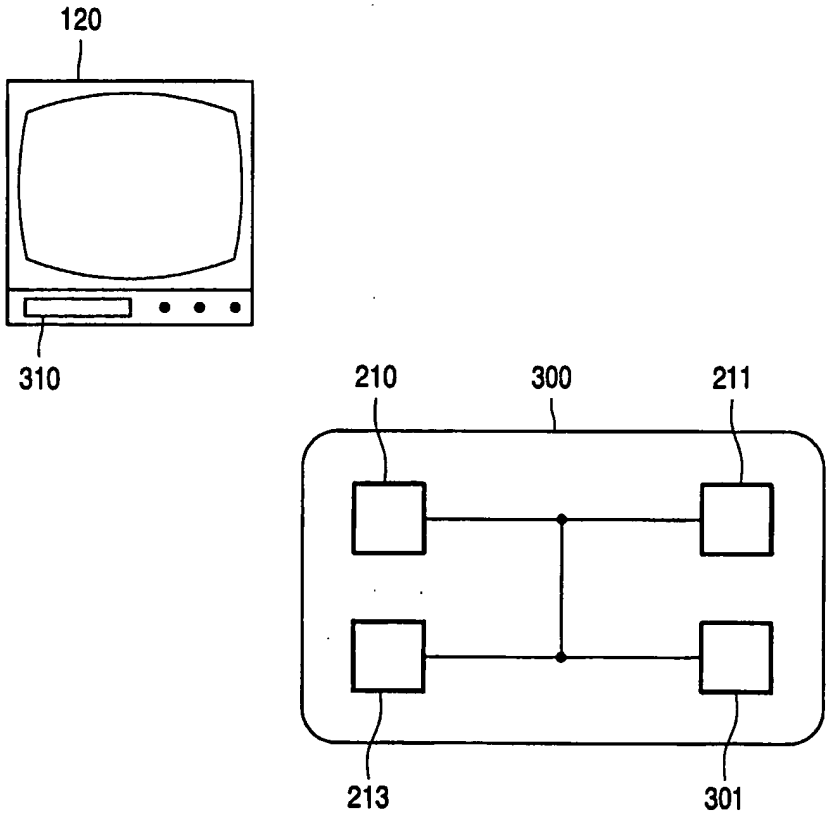
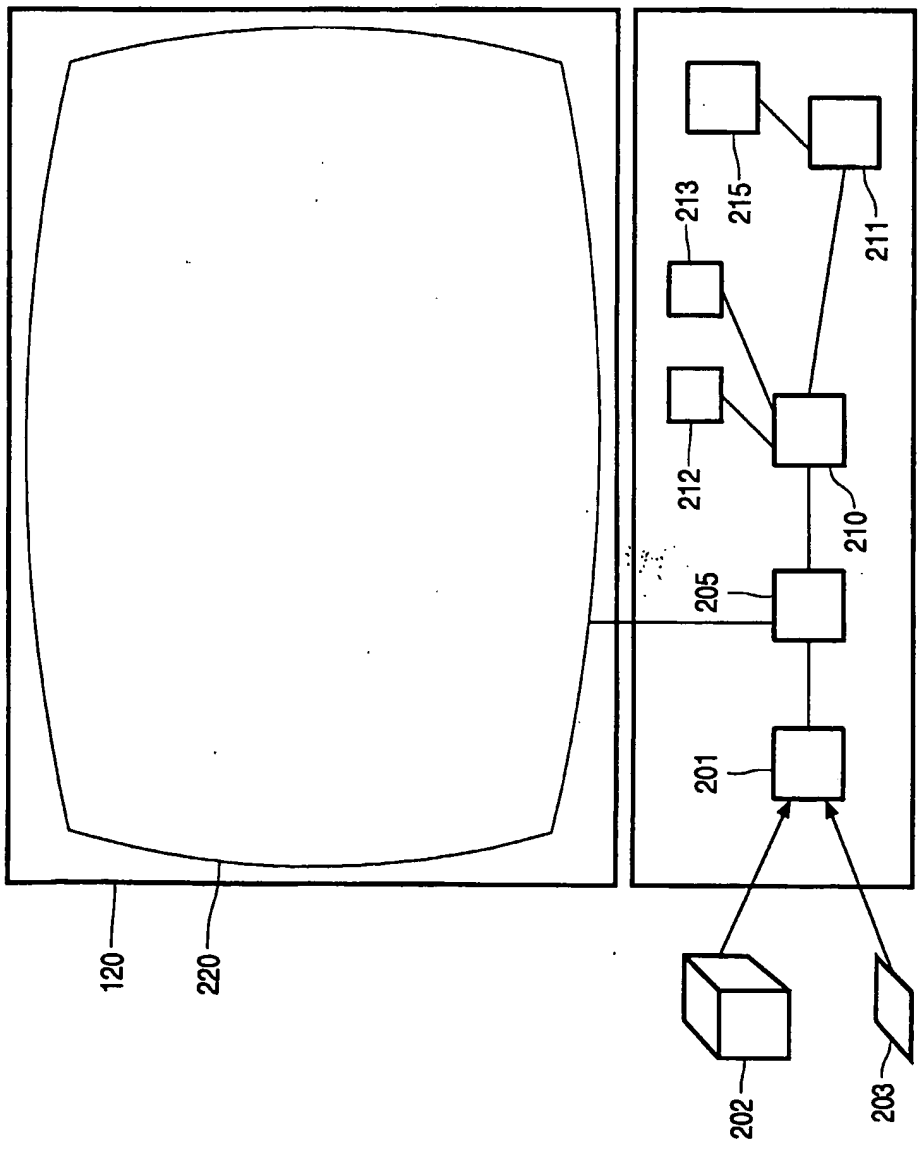


FIG. 3

FIG. 2



INTERNATIONAL SEARCH REPORT

	Ional Application No
	PCT/IB 02/02138

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 094 667 A (IRDETO ACCESS BV) 25 April 2001 (2001-04-25)	1,7
A	the whole document	2-6,8,9

Y	WO 88 06826 A (MARS INC) 7 September 1988 (1988-09-07)	1,7
A	the whole document	2-6,8,9

A	US 6 035 329 A (FENG JIE ET AL) 7 March 2000 (2000-03-07) abstract	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2002	26/07/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Greve, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

nformation on patent family members

I ional Application No
PCT/IB 02/02138

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1094667 A	25-04-2001	EP 1094667 A1	25-04-2001
		AT 217136 T	15-05-2002
		AU 7663400 A	30-04-2001
		BR 0014842 A	11-06-2002
		DE 69901398 D1	06-06-2002
		WO 0130082 A1	26-04-2001
WO 8806826 A	07-09-1988	EP 0304458 A1	01-03-1989
		WO 8806826 A1	07-09-1988
		JP 2500316 T	01-02-1990
US 6035329 A	07-03-2000	US 5892825 A	06-04-1999
		AU 5259898 A	22-06-1998
		EP 0974217 A2	26-01-2000
		WO 9824037 A2	04-06-1998
		AU 1280397 A	27-06-1997
		WO 9721167 A1	12-06-1997
		US 5937164 A	10-08-1999
		US 6185306 B1	06-02-2001